AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

SUMQAYIT DÖVLƏT UNİVERSİTETİ

FAKÜLTƏ: ***MÜHƏNDİSLİK***

KAFEDRA: ***İNFORMASİYA VƏ KOMPÜTER TEXNİKASI***

İXTİSAS: ***KOMPÜTER MÜHƏNDİSLİYİ***

KOMPÜTER SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİ FƏNNİNDƏN

LABORATORİYA İŞLƏRİ ÜÇÜN TƏLİMAT

TƏRTİB ETDİ: **ASS. ALLAHVERDİYEVA K.Ə.**

SUMQAYIT - 2016

"Təsdiq edirəm"
"İnformasiya və KT" kafedrasının müdiri
_____ dos. Mənsurov Q.M.
"_____"_____ 2020-ci il

Mühəndislik fakültəsi, Bakalavr təhsili pilləsi, qrup-611 (2), kurs II
050631-Kompüter mühəndisliyi ixtisası,
Kompüter sistemlərinin təhlükəsizliyi (İPF-B10, 4 kredit) fənni üzrə
Təqvim-tematik plan (laboratoriya 15 saat)

№	Tədris olunacaq mövzular	Tarix	Saat
1	***2***	***3***	***4***
1.	Təhlükəsizlik texnikası və laboratoriya işləri ilə tanışlıq. Kompüter şəbəkələrində təhlükələrin təsnifatı. İnformasiya təhlükəsizliyi.	20.02.2020 05.03.2020	4
2.	Kompüter sistemlərinin təhlükəsizliyi və online təhlükəsizlik.	19.03.2020 02.04.2020	4
3.	Kriptoqrafiya. Simmetrik və assimmetrik şifrələmə. İnkar edilə bilən şifrələmə.	16.04.2020 30.04.2020	4
4.	Kompüter virusları. Antivirus proqramları vasitəsilə informasiyanın mühafizəsi.	14.05.2020	2
5.	İnformasiyanın arxivləşdirilməsi və ehtiyyat surətinin yaradılması sistemləri.	28.05.2020	1

Ədəbiyyat

1. Qasımov V.A. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyat-Poliqrafiya Mərkəzi. 2009, 340 s.

2. Əlizadə M. N., Bayramov H.M., Məmmədov Ə. S. İnformasiya Təhlükəsizliyi, Dərslik, Bakı, "Iqtisad Universiteti" nəşriyyatı, 2016, 384 səh.

3. Laboratoriya işinə aid təlimatlar.

Fənn müəllimi: b/m.K.Ə.Allahverdiyeva

LABORATORIYA İŞİ №1
KOMPÜTER ŞƏBƏKƏLƏRİNDƏ TƏHLÜKƏLƏRİN TƏSNİFATI

İŞİN MƏQSƏDİ: Bu işdə əsas məqsəd Kompüter şəbəkələrində yarana biləcək bütün təhlükələri araşdırmaqdan ibarətdir.

NƏZƏRİ HİSSƏ

Təhlükə dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyişdirilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
- Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).
- Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.
- Bütövlük - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.
- Əlyetənlik – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.
- Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:
- Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
- Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
- Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
- Təsir xarakterinə görə (aktiv, passiv);
- Obyektə münasibətinə görə (daxili, xarici).
- Lokal kompüter şəbəkələri (LKŞ)-nin əsas aparat komponentləri kimi aşağıdakılardan istifadə edilir:
- İşçi stansiyalar;
- Serverlər;
- İnterfeys plataları;
- Kabellər.
- İşçi stansiyalar (İST) – şəbəkə istifadəçisinin iş yeri kimi istifadə olunan
- fərdi kompüterlərdir. İST – nin tərkibinə olan tələbat şəbəkədə həll olunan məsələlərin xarakteriskaları, hesablama proseslərinin təşkil olunma prinsipi, istifadə olunan ƏS və bir sıra digər amillərlə təyin olunur. Məsələn, əgər şəbəkədə MS Windows for Workgroup ƏS – dən istifadə edilirsə, o zaman İST – nin prosessoru kimi Pentium tipli prosessorlardan istifadə etmək lazımdır.
- Bəzi hallarda İST birbaşa şəbəkə kabelinə qoşulmuş olursa, bu halda maqnit disklərində yaddaşa ehtiyac qalmır.Bu cür İST disksiz İST adlanırlar. Lakin bu halda fayl – serverdən İST -ə ƏS yükləndikdə, şəbəkə adapterində uzaq məsafədən yükləməyə imkan verən uyğun mikrosxem olmalıdır. Bu mikrosxem girş – çıxış baza sisteminin (BİOS) genişlənməsi kimi istifadə olunur. Bu mikrosxemdə İST – nin əməli yaddaşına ƏS – nin yüklənməsi proqramı yazılır. Bu cür disksiz İST-in əsas üstün cəhəti onların ucuz olması və burada istifadəçinin

proqramına icazə verilmədən daxil olmanın mümkünsüzlüyü və kompüter viruslarının daxil ola bilməməsidir. Mənfi cəhəti isə onun avtonom rejimdə işləyə bilməməsi (serverə qoşulmamaq şərtilə), həmçinin özünün verilənlər və proqram arxivinin olmamasıdır.

- LKŞ – də serverlər – şəbəkə resurslarını paylamaq funksiyasını yerinə yetirirlər. Adətən server funksiyasını kifayət qədər güclü olan fərdi kompüter, meynfreym və ya xüsusi kompüter həyata keçirə bilər. Hər bir server həm ayrıca, həm də İST tərkibində ola bilər. Axırıncı halda serverin tam deyil, yalnız resurslarının bir hissəsi ümumi istifadədə ola bilər.
- LKŞ – də bir neçə server olarsa, o zaman hər bir server ona qoşulan İST -ə xidmət göstərir. Serverin kompüterlər toplusuna və onlara qoşulmuş İST-ə domen dyilir. Bəzi hallarda bir domendə bir neçə server olur. Bu serverlərdən biri baş server, qalanları isə ehtiyat serveri və ya əsas serverin məntiqi genişlənməsi rolunu oynayırlar.
- Kompüter server tipini seçdikdə əsas parametr kimi prosessorun tipi, əməli yaddaşın tutumu, sərt diskin tipi və tutumu, disk kontrollerinin tipi nəzərə alınmalıdır. Bu xarakteriskaların qiymətləri həll olunacaq məsələdən, şəbəkədə hesablamaların təşkil olunmasından, şəbəkənin yüklənmə dərəcəsindən, istifadə olunan ƏS-dən və digər amillərdən asılıdır.
- Serverdə əməli yaddaş nəinki öz proqramını yerinə yetirmək məqsədini güdür, həmçinin disk giriş – çıxışının buferlərini yerləşdirmək məqsədi üçün də istifadə edilir. Buferlərin optimal sayını təyin etməklə, giriş-çıxış əməllərinin yerinə yetirilmə sürətini artırmaq olar.
- Əməli yaddaşı seçdikdə nəzərə almaq lazımdır ki, orada lazımi proqram təminatı, həmçinin şərikli istifadə olunan fayllar və verilənlər bazaları yerləşməlidir.
- İST və serverlər şəbəkənin yerləşdiyi yerlərdə öz aralarında kabel şəklində olan verilənlərin ötürülmə xətti ilə birləşirlər. Kompüterlər kabelə interfeys palatası – şəbəkə adapteri vasitəsilə birləşdirilir. Son zamanlar verilənlərin ötürülmə mühiti kimi istifadə olunan xətsiz şəbəkələr – radiokanallar meydana gəlmişdir.
- Bəzi hallarda kompüterlər bir neçə qonşu otaqlarda yerləşdirilir.
- İstifadə olunan şəbəkə adapteri 3 əsas xarakteriskaya malikdirlər: kompüterin qoşulduğu şinin tipi (İSA, EISA, Micro Channel və s.) mərtəbələr şəbəkəsinin sayı (32,64) və yaradılan şəbəkənin topologiyası (Ethernet, Arcnet, Token - Ring). Məs. Ethernet topologiyalı və Novell Net Ware və ya MS Windowsfor Workgropus ƏS-ə malik şəbəkələr üçün Novell firmasının NE3200 (32 bitli) şəbəkə adapterindən istifadə etmək daha məqsədə uyğun sayılır.
- Şəbəkə kabelinin seçilməsi onun spesifikasiyası ilə əlaqədar olub, şəbəkə adapterinin sənədlərində göstərilir.
- LKŞ-ın əlavə avadanlıqlarına fasiləsiz qida mənbələri, modemlər, transirverlər, repiterlər və müxtəlif kontaktlar sistemi kimi istifadə olunan konnektorlar və terminatporlar daxildirlər.
- Fasiləsiz qida mənbələri (UPS-Unit Power System) – elektrik şəbəkəsinin dayanıqlı işləməsini artırır və elektrik şəbəkəsi açıldıqda serverdə olan verilənlərin itməməsini təmin edir. Dövrədə kompüteri qidalandıran gərginlik açılarsa, o zaman kompüter öz işinə UPS sayəsində davam edəcək, kompüterin əməli yaddaşına yüklənmiş proqram və verilənlər itməyəcək. UPS-i seçdikdə fikir vermək lazımdır ki, onun gücü serverlərin gücündən az olmasın.
- Transiver – İST –ni yoğun koaksil kabelinə qoşan qurğudur.
- Repiter – isə şəbəkə seqmentlərini birləşdirən qurğudur.
- Konnektorlar (birləşdiricilər) kompüterlərin şəbəkə adapterlərini nazik kabellə birləşdirmək üçündür.
- Terminatorlar – açıq kabellərə şəbəkənin qoşulması üçün, həmçinin torpaqlama məqsədilə də istifadə oluna bilər.
- Modem – telefon xətti vasitəsilə LKŞ və ya ayrıca kompüteri qlobal şəbəkəyə qoşan qurğudur.
- Elementlərin şəbəkəyə qoşulma konfiqurasiyalarına topologiya deyilir. Topologiya şəbəkənin bir sıra vacib xarakteriskalarını,o cümlədən etibarlı işləməsini, məhsuldarlığını, dəyərini, mühafizə olunmasını təyin edir.
- LKŞ topologiyasının təsnifatına yanaşmalardan biri topologiyanı 2 əsas sinfə bölməkdir: genişyayılmış və ardıcıl tipli.

- Genişyayılmış topologiya konfiqurasiyasında hər bir kompüterin ötürdüyü siqnal yerdə qalan kompüterlər tərəfindən qəbul olunur. Bu cür konfiqurasiyaya “ümumşin”, “ağacabənzər”, “passiv mərkəzli ulduz” topologiyalarını aid etmək olar.
- Ardıcıl konfiqurasiyalı topologiyada isə hər bir fiziki alt-səviyyə informasiyanı yalnız bir fərdi kompüterə verə bilir. Buna misal olaraq ixtiyari (kompüterlər bir – birilə ixtiyari şəkildə birləşirlər), “iyerarxik”, “halqavari”, “zəncirvari”, “intellektul mərkəzli ulduz”, “qar dənələri şəklində” və s.
- topologiyalarını göstərmək olar.
- LKŞ topologiyasının geniş yayılmış 3 növünü nəzərdən keçirək:
- Mərkəzi qovşaq kimi, passiv birləşdirici və ya aktiv təkrarlayıcıdan istifadə edilə bilər. Bu topologiyanın mənfi cəhəti onun etbarlılığının az olmasıdır, çünki mərkəzi qovşaq işdən çıxan kimi, bütün şəbəkə öz işini dayandırır və həmçinin burada çox böyük uzunluqlu kabeldən istifadə edilir. Bəzi hallarda işləmə etibarlılığını artırmaq üçün mərkəzi qovşaqda xüsusi rele qoyulur ki, bunun vasitəsilə sıradan çıxmış kabellər dövrədən açılır.
- “Ümumişin” topologiyasında bütün kompüterlər bir kabelə qoşulurlar. Burada informasiya kompüterlərə növbə ardıcıllığı ilə verilir.
- Bu halda uzunluğu kiçik olan kabeldən istifadə edilir, “ulduz” topologiyasına nəzərən daha etibarlı işləyir, çünki ayrı-ayrı kompüterlərin işdən çıxması, şəbəkənin ümumi işinə xələl gətirmir. Mənfi cəhəti ondan ibarətdir ki, əsas kabel zədələndikdə bütün şəbəkə öz işçi funksiyasını itirir; həmçinin burada bir kompüterdən digərinə göndərilən informasiya başqa kompüterlər tərəfindən də qəbul oluna bildiyi üçün fiziki səviyyədə informasiya zəif mühafizə olunur.
- “Halqavari” topologiyada bir kompüterdən digərinə verilənlər “estafet” də olduğu kimi ötürülür
- Əgər hər hansı bir kompüter ona aid olmayan verilənləri qəbul edibsə, o zaman həmin kompüter o verilənlərin halqavari istiqamətdə o biri kompüterlərə ötürəcəkdir.
- Bu topologiyanın üstün cəhəti, kabel sıradan çıxan zaman sistemin iş qabiliyyətinin saxlanmasıdır. Çünki, bu halda hər bir kompüterə daxil olmanın iki yolu olur. Mənfi cəhəti isə kabelin müəyyən qədər uzun olması, “ulduz” – a nisbətən sürəti kiçik olması, həmçinin “ümumi şin” topologiyasında olduğu kimi, informasiyanın zəif mühafizə olunmasıdır.
- Real LKŞ – nin topologiyası yuxarı da göstərilən topologiyalardan və ya onların kombinasiyalarından birinin əsasında qurula bilər. Ümumi halda şəbəkənin strukturu aşağıdakı amillərlə təyin olunur: birləşdirilən kompüterlərin sayı, informasiyanın ötürülməsinin operativliyi və etibarlılığı, iqtisadi amillər və s.
- Lokal şəbəkələrdə mərkəzləşdirilmiş və mərkəzləşdirilməmiş kimi 2 əsas idarə prinsipi mövcuddur.
- Mərkəzləşdirilmiş idarəetmədə verilənlər mübadiləsinin idarəsi fayl – serstansiyaları tərəfindən istifadə edilə bilərlər. Bir işçi stansiyasının faylına digər işçi stansiya müraciət edə bilməz. Əsas daxil olma yolundan istifadə etməməklə, “Net Link” proqramı vasitəsilə işçi stansiyalar arasında fayllar mübadiəsini təşkil etmək olar. Bu proqramın icrası ilə NC proqramında faylı köçürdüyümüz kimi, iki kompüter arasında faylları bir – birinə ötürmək olar.
- Mərkəzləşdirilmiş idarəli şəbəkənin üstün cəhəti şəbəkə resurslarının onlara icazəsiz daxil olmaların yüksək dərəcədə mühafizəsi, daha böyük saylı qovşaqlara malik şəbəkələrin qurulmasının mümkünlüyüdür. Mənfi cəhəti isə, fayl-server öz iş qabiliyyətini itirdikdə, sistemə icazəsiz daxil olmanın mümkünlüyü, həmçinin server resurslarına daha yüksək tələblərin olmasıdır.
- Mərkəzləşdirilməmiş (bir səviyyəli) şəbəkələrdə xüsusi ayrılmış serverlər olmur. Şəbəkənin idarəetmə funksiyası növbə ilə bir İST – dən digər İST – yə ötürülür. Bir İST-nin resurslarından (disklər, printerlər və digər qurğular) digər İST istifadə edə bilər. Bu cür şəbəkələrdə Windows ƏS-dən istifadə etmək olar.
- Çox da böyük olmayan İST üçün bu cür şəbəkə daha səmərəlidir və real paylanmış hesablama mühitinin qurulmasına imkan verir. Mərkəzləşdirilmiş şəbəkələrə nəzərən burada proqram təminatı daha sadə olur. Burada fayl-serverdən istifadə edilməsi lazım olmur, bu da sistemin daha ucuz yaranmasına səbəb olur. Lakin bu şəbəkədə informasiyanın mühafizəsi və inzibati idarə məsələləri bir qədər zəif alınır.

- Kompüterlər arasında informasiya mübadiləsini təşkil etmək məqsədilə LKŞ-də Elektrotexnika və Radiotexnika sahəsində Beynəlxalq İnstitut (İEEE – İnstute of Electrical and Electroncal Engineers) tərəfindən hazılanmış standart protokollardan istifadə olunur.
- İEEE802.3 və İEEE802.4 standartlarında təsvir edilən və lokal şəbəkələrdə (Ethernet, Arcnet və Token Ring) istifadə olunan mübadilə protokollarına qısa nəzər salaq. Bu protokollar vasitəsilə şəbəkə kanal verilənlərinə daxil olma üsulları götərilir. Bunlar OSI modelinin kanal səviyyəsini hayata keçirirlər.
- "Ethernet" üsulu. Bu Xerox firması tərəfindən təklif edilmiş və burada "ümum şin" topologiyasından istifadə edilmişdir. Ümumi şin ilə ötürülən məlumatların sərlövhəsində ötürülən və qəbul edən mənbələrin ünvanları göstərilir.
- Bu üsul aparıcı tezliyi araşdırmaq və ziddiyitləri yox etməklə, çoxşahəli mübadilə üsuludur (CSMA/CD – Caries Sense Multiple Access with Collision Delection). Bu üsulun mahiyyəti ondan ibarətdir ki, İST yalnız o vaxt məlumatı ötürməyə başlayır ki, kanal boş olsun, əks təqdirdə məlumatın ötürülməsi müəyyən zaman anı üçün gecikdirilmiş olacaq. Eyni zamanda verilənlərin ötürülmə imkanı avtomatik olaraq aparat üsulu ilə həyata keçirilir.
- 80-100 İST eyni vaxtda işlədikdə şəbəkənin işləmə sürəti azlır. Bu, kanalda əmələ gələn münaqişələrlə əlaqədardır.
- "Arenet" üsulu – Datapoint Corp. Firması tərəfindən təklif edilmiş və burada "ulduz" topologiyasından istifadə olunmuşdur. Bu halda bir İST –dən digər iST -ə məlumatların ötürülməsi İST-in birində təşkil edilən markerlər vasitəsilə həyata keçirilir. Məlumat ötürmək istəyən İST markerin ona gəlməsini gözləyir, göndərənin və qəbuledilənin ünvanları yazılmış sərlövhəyə malik məlumatı buna birləşdirir. Əgər İST qəbulu gözləyirsə , yenə də markerin gəlməsini gözləməlidir. Marker gəldikdən sonra məlumatlarla birlikdə gələn sərlövhə anaıiz olunmalıdır. Əgər alınan məlumatlar bu İST-ə aid olarsa,o zaman İST onu markerdən ayırır.
- "Arcnet" şəbəkəsinin avadanlıqları "Ethernet" və "Token Ring" şəbəkələrinə nəzərən daha ucuz olurlar, lakin həmin avadanlıqların etibarlılığı və məhsuldarlılığı nisbətən aşağı olur.
- "Token Ring" üsulu - "halqavari" topologiyaya malik olub İBM firması tərəfindən təklif edilmişdir. Bu firmadan başqa, bu cür şəbəkələrin avadanlıqlarını Proteon, 3 Com və Undermann - Bass firmaları, şəbəkə proqram təminatını isə 3COM, Novell və Univation firmaları istehsal edirlər. Bu üsul "Arcnet" üsuluna oxşayır. Əsas fərq ondan ibarətdir ki, burada üstünlük mexanizmi vardır. Bunun sayəsində bəzi İST digərlərinə nəzərən daha tez markeri əldə edə bilirlər və onu bir qədər özündə saxlamaq imkanına mail olurlar.
- LKŞ -də tipik proqramlardan istifadə etmək məqsədilə şəbəkədə məlumatların mübadiləsi üçün hansı protokoldan istifadə olunmasını bilmək lazımdır. Belə protokollardan bir neçəsi mövcuddur. Ən geniş yayılmış protokollar bunlardır.
- İPX, SPX və NETBİOS.
- İPX (İnternetwork Packet Exchange) – protokolu OSI modelinin nəqliyyat səviyyəsinin protokoludur. O, şəbəkənin aşağı səviyyələri ilə interfeysə malikdir.
- SPX (Sequenced Packet Exchange) - daha yüksək səviyyə olan seans səviyyəsinin protokoludur. O, İPX, NETBİOS (Network Basic İnput/ Output System – şəbəkə giriş-çıxış baza sistemi) protokolları əsasında yaradılmışdır. Bunun vasitəsilə OSI modelinin şəbəkə, nəqliyyat və seans səviyyələrinin funksiyaları həyata keçirilir.

YOXLAMA SUALLARI

1. Lokal şəbəkə dedikdə nə başa düşürsünüz?
2. "Arenet" üsulu dedikdə nə başa düşürsünüz?
3. "Ethernet" üsulu dedikdə nə başa düşürsünüz?

LABORATORİYA İŞİ №2
İNFORMASİYA TƏHLÜKƏSİZLİYİ

İŞİN MƏQSƏDİ: Bu işdə əsas məqsəd informasiya təhlükəsizliyinin təmin olunması məsələlərini tədqiq etməkdən ibarətdir.

NƏZƏRİ HİSSƏ

İnformasiya təhlükəsizliyi (Information Security, Информационная безопасность) – informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli, təsadüfi və ya qəsdli təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəli olmasıdır.

İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

Təhdid dedikdə kiminsə maraqlarına ziyan vurmağa səbəb ola bilən potensial mümkün hadisə, şərait, hərəkət, proses və s. nəzərdə tutulur.

Təhlükə dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyişdirilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
- Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service – xidmətdən imtina).
- Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.
- Bütövlük – informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.
- Əlyetənlik – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:

- Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
- Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
- Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
- Təsir xarakterinə görə (aktiv, passiv);
- Obyektə münasibətinə görə (daxili, xarici).

Daxili və xarici təhlükələrin nisbətini təqribi olaraq belə xarakterizə etmək olar. Təhlükələrin 80%-i təşkilatın öz işçiləri tərəfindən onların bilavasitə və ya dolayısı yolla iştirakı ilə baş verir. Təhlükələrin 20%-i kənardan icra olunur.

İnformasiya təhlükəsizliyinin üç aspekti mövcuddur.

1. *əlyetənlik* − yolverilən vaxt ərzində tələb olunan informasiya resursunu, informasiya xidmətini əldə etmək imkanı;
2. *tamlıq* − informasiyanın əvvəlcədən müəyyən edilmiş şəkil və keyfiyyəti saxlaması xassəsi;

3. *konfidensiallıq* − informasiyanın icazəsiz girişlərdən məxfi saxlanılması xassəsidir.

İnformasiyanın bu xassələrindən çıxış edərək təhdidlərin üç əsas növünü ayırmaq olar:

- konfidensiallığın pozulmasına yönələn təhdidlər;
- əlyetənliyin pozulmasına yönələn təhdidlər;
- tamlığın pozulmasına yönələn təhdidlər.

- **DoS-hücum** (ing. *Denial of Service* − xidmətdən imtina) veb-saytın, veb-serverin və digər şəbəkə resursunun normal işini pozmaq və ya çətinləşdirmək məqsədilə həyata keçirilir. Bu hücumları müxtəlif üsullarla həyata keçirirlər. Üsullardan biri serverə çoxsaylı sorğuların göndərilməsidir, serverin resursları onların emalı üçün yetərli olmadıqda serverin işi çətinləşə və ya pozula bilər.
- DDoS (Distributed Denial of Service − paylanmış xidmətdən imtina) hücumunda şəbəkə resurslarına bir deyil, çox sayda kompyuterdən sorğular göndərilir. Yoluxdurulmuş kompyuterlərdən biri "idarəetmə mərkəzi" kimi istifadə edilir, o "zombi" adlandırılan digər kompyuterlərdən edilən hücumları idarə edir.[1]
- **Botnet** (ing. *botnet* termini *robot* və *network* sözlərindən yaranmışdır) − bəd niyyətliyə istifadəçinin xəbəri olmadan yoluxmuş kompyuteri məsafədən idarə etməyə imkan verən ziyankar proqramlarla − botlarla yoluxmuş kompyuterlərdən ibarət şəbəkədir. Bot istifadəçinin kompyuterində gizli quraşdırılan və bədniyyətliyə yoluxmuş kompyuterin resurslarından istifadə etməklə müəyyən əməlləri yerinə yetirməyə imkan verən proqramdır.
- Botnetlər adətən spam göndərilməsi, konfidensial informasiyanın toplanması, xidmətdən imtina hücumları (Dos-hücum),fişinq üçün istifadə edilir.[1]
- **Fişinq** (ingiliscə:"Fishing", rusca:"Фишинг") – ingilis dilindən tərcümədə "balıq ovu" deməkdir və qlobal şəbəkədə balıq ovunu xatırladan fırıldaqçılığın bir növüdür. Belə ki, fırıldaqçı (fişer) İnternetdə "tələ" quraraq, bu tələyə düşən İnternet istifadəçilərini aldatmaqla məşğuldur. Fişer müxtəlif üsullarla İnternet istifadəçilərindən bank hesablarını, kredit kartlarını və İnternetə çıxış üçün lazım olan informasiyaları öyrənir.
- Fişinq kiberdələduzluğun xüsusi növüdür, istifadəçiləri aldatma yolu ilə adətən maliyyə xarakterli fərdi məlumatları təqdim etməyə məcbur etməyə yönəlir. Dələduz bank saytı kimi görünən (və ya maliyyə əməliyyatları aparılan istənilən digər sayt kimi, məsələn, eBay) saxta veb-sayt yaradır. Sonra cinayətkarlar istifadəçiləri bu sayta aldadıb aparmağa cəhd edirlər ki, bu saytda onlar login, parol və ya PIN-kod kimi konfidensial məlumatları daxil etsinlər. Çox zaman dələduzlar bunun üçün həmin saytlara istinadları spamın köməyi ilə yayırlar.

YOXLAMA SUALLARI

1. İnformasiyanın mühafizəsi dedikdə nə başa düşürsünüz?
2. İnformasiya təhlükəsizliyinin hansı aspektləri mövcuddur?
3. DoS-hücum anlayışını izah edin.
4. Fişinq hücum anlayışını izah edin.
5. Botnet hücum anlayışını izah edin.

LABORATORİYA İŞİ №3
Kompüter sistemlərinin təhlükəsizliyi və onlayn təhlükəsizlik

İŞİN MƏQSƏDİ: Bu işdə əsas məqsəd kompüter sistemlərinin təhlükəsizliyi ilə tanış olmaq və tədqiq etməkdən ibarətdir.

Kompüter təhlükəsizliyi, kompüter istifadə etdiyiniz zaman ortaya çıxa biləcək risklərin idarə edilməsi ilə maraqlanan kompüter elmi sahəsidir. Çox təəssüf ki kompüterlərin məlumatsız və diqqətsiz istifadəsi maddi və mənəvi zərərlərlə nəticələnir. Bu zərərlərdən qaçmaq üçün bəzi təməl mövzuları bilmək və bəzi təhlükəsizlik tədbirlərini almaq lazımdır.

Risklər hardan gələbilər? Kompüter istifadəsindən qaynaqlanan risklər, müxtəlif şəkillərdə ortaya çıxar. Işlətdiyimiz proqramlarda tapılması olabiləcək açıqlar və səhvlər, bunlara yerləştirlmiş ola biləcək arxa qapılar, zərər vermə məqsədiylə yazılmış virus və bənzəri proqramları, pis niyyətli kəslərin edə biləcəyi birbaşa və dolayı hücumları, yalan cəhdləri və istifadəçi səhvləri bunlara örnəkdir. Hansı qaydalara əməl etmək vacibdir?

1. KOMPÜTERİNİZİ YENİLƏNMƏYƏ AÇIQ SAXLAYIN

Əməliyyat sistemlərində və proqramlarda kompyuterinizə zərər verəcək açıqlar və səhvlər ola bilər. Bu açıqlar, pis niyyətli kəslər tərəfindən tapılsa kompüterinizin yavaşlaması, səhv verməsi, istəmədiyiniz şeylər etməsi, şəxsi məlumatlarınızın oğurlanma, məlumat itkiləri kimi istənməyən nəticələr meydana gələ bilər. Proqram istehsalçıları, öz məhsullarındakı səhvlərin

fərqinə vardıqda bunları düzəltməyə çalışırlar. Bu səbəblə tez-tez əməliyyat sistemlərinin və digər proqramların səhv düzəltmələri ehtiva edən yeni versiyaları çıxır. Buna görə kompyuterinizin aktual qalması əhəmiyyətlidir. Kompüterinizi aktual tuta bilmək üçün avtomatik yeniləmə proqramlarını aktiv hala gətirməli, nizamlı olaraq istifadə etdiyiniz proqramların aktual distributivlərinin çıxıb çıxmadığını nəzarət etməlisiniz. Windows əməliyyat sistemi yeniliklərinin update.microsoft.com ünvanından təqib edə bilərsiniz. Hər hansı bir Linux paylamas istifadə, əməliyyat sistemi ilə yanaşı istifadə etdiyiniz bütün digər proqramların yeniliklərinin, paket idarəçisi proqramlarından tək basma ilə edə bilərsiniz.

2. TƏHLÜKƏSİZ PROQRAMLAR SEÇİN

Hər kompüter proqramı eyni nisbətdə etibarlı deyil. Bəzi proqramlar, digərlərinə görə həddindən artıq səhv / açıq ehtiva edirlər. Hətta bəzi proqramlar, yalnız başqa kompüterlərə zərər vermək məqsədilə yazılmışdır. Bu səbəblə etibarlı proqramları seçmək vacibdir. Ümumi olaraq, böyük açıq qaynaq kodlu proqram layihələri, bir çox adam tərəfindən inkişaf etdirilib denetlenebildiğinden daha az təhlükəsizlik açığı ehtiva edərlər. Siz də etibarlı proqramlar istifadəyə Firefox və Thunderbird ilə başlaya bilərsiniz. Windows əməliyyat sisteminin risklərini tamamilə uzaqlaşmaq üçün Linux əsaslı əməliyyat sistemlərini kullanabilirsiniz. Misal üçün Pardus, Tübitak UEKAE tərəfindən inkişaf etdirilən asan istifadə edilə bilər, Türkçe bir Linux dağıtımının.

2. VİRUSLARDAN QORUNMA PROQRAMLARINDAN İSTİFADƏ EDİN

Virus, soxulcan (worm), truva atı (trojan) kimi proqramlar, kompüterlərə zərər verə biləcək proqramlardır. Müxtəlif qaynaqlardan kompüterinizə bu cür zərərli proqramlar bulaşa bilər. Bu bir disket, CD, DVD və ya USB disk ilə ola bilər. Ancaq şübhəsiz İnternet, zərərli proqramların dağılması üçün ən böyük mənbədir. Xüsusilə ölkəmizdə get-gedə yayılan ADSL və ya KabloNet vasitəsilə davamlı bir İnternet bağlantısına sahibsinizsə risk daha böyükdür. Virus və bənzəri proqramların kompüterinizə zərər verməsinin qarşısını almaq üçün virusdan qorunma (antivirus) proqramlarından istifadə lazımdır. Bu proqramlardan istifadə etdiyiniz kompüterinizi tamamilə qoruyaraq zərərli proqramları tapıb təmizləyə biləcəkləri kimi, davamlı arxa planda çalışaraq gələn bir təhlükəni anında idarə altına ala bilərlər. Hər gün təxminən üç yeni virus ortaya çıxmaqda və təhlükəli viruslar ortaya çıxmalarından etibarən bir neçə saat içində çox sürətli bir şəkildə yayılmaqdadır. Yeni viruslara qarşı qorunmaq üçün aktual virus məlumatlarına sahib olmaq lazımdır. Bu səbəblə bu proqramları çıxaran firmalar gündə / həftədə bir neçə dəfə virus məlumatı olan verilənlər bazalarını yenilərlər. Virusdan qorunmaq proqramları istifadə edən insanların bilməsi lazım olan ən əhəmiyyətli şey, bu proqramların tez-tez yenilənməsi lazım olduğudur. Virus və digər zərərli proqramlardan qorunmaq üçün ödənişli antivirus proqramları istifadə edə biləcəyiniz kimi Antivir, Avast, AVG, ClamAV kimi müvəffəqiyyətli nişan da istifadə edə bilərsiniz. Windows xaricindəki əməliyyat sistemlərində isə (MacOS, Linux, Solaris, BSD və s.) kompüterinizə zərər verə biləcək aktiv viruslar olmadığı üçün antivirüs proqramları istifadə etməyinizə ehtiyac qalmaz.

4. TƏHLÜKƏSİZLİK DİVARI İSTİFADƏ EDİN

İnternet üzərindən bir kompüterə hücum reallaşdırmaq istəyən insanlar, qarşıdakı kompüterlərdə açıq bir əlaqə nöqtəsi axtarırlar. Belə bir əlaqə nöqtəsi tapmaları halında, xüsusi məlumatlarınızı, şifrələrinizi, kredit kartı nömrənizi ələ keçirə bilər; kompüterinizi qanunsuz işlər üçün istifadə edə bilər, sisteminizə zərər verə bilərlər. Veb skanerləri, e-poçt proqramları, anında mesajlaşma proqramları, çox oyuculu oyunlar və əməliyyat sistemlərində müsbət bir özellikmiş kimi görünən bəzi xidmətlər asan kırılabilen bir əlaqə nöqtəsi yarada. Açıq əlaqə nöqtələrini bağlayaraq çöldən gələn hücumları qarşısını almaq və kompüterinizdə icazə vermədiyiniz proqramların İnternetə əlaqələrini önləmək üçün təhlükəsizlik divarı (firewall) adı verilən proqramları istifadə edilə bilər. Məsələn, Windows XP istifadəçiləri Service Pack 2 yeniləməsini yükləyərək, pulsuz bir təhlükəsizlik divarına sahib ola bilərlər. Təhlükəsizlik duvarınızın aktiv vəziyyətdə olub olmadığından əmin olmaq üçün Yoxlama Masasındaki Windows Təhlükəsizlik Mərkəzini ziyarət edilə bilər.

5. ETİBAR ETMƏDİYİNİZ İNTERNET SAYTLARINA DİQQƏT EDİN

Yuxarıda qeyd olunduğu kimi, kompüterlə əlaqədar təhlükəsizlik risklərinin böyük hissəsi İnternet qaynaqlıdır. Bilinməyən İnternet saytlarını ziyarət edən istifadəçilər, zərərli kodlar ehtiva edən web tətbiqlərini işlədərək ya da virus saxlayan faylları kompüterlərinə endirərək kompüterlərinə zərər verə bilərlər. Xüsusilə qeyri-qanuni məzmunlu saytlar (Hack, Crack, Warez, Porno vs.) Sizin kompüterinizə zərər verməkdən də çəkinməyəcəklər. Bu səbəblə veb skanerlərin təhlükəsizlik xəbərdarlıqlarını diqqətsizcə «bəli» deyərək keçmək, hər əlaqəyə (link) şüursuzca basmaq, hər faylı yükləməyə çalışmaq, qaçınılması lazım olan davranışlardır.

6. POÇT ÜNVANINIZA GƏLƏN TANIMADIGINIZ MƏKTUBLARI VƏ FAYLLARI AÇMAYIN

Təhlükəsizlik belə təmin edilməz:) Virusların və digər zərərli proqramların özlərini paylamaq üçün ən çox üstünlük etdikləri üsul e-poçt göndərməkdir. Tanımadığınız kəslərdən gələn, başlıqları şübhəli olan və əlavə fayl (attachment) ehtiva edən e-poçtların virus olma ehtimalları yüksəkdir. Belə hallarda e-məktubun açılmadan silinməsi lazımdır. E-poçt və ya anında mesajlaşma proqramları vasitəsilə (MSN Messenger, ICQ, GTalk və. s) tanıdığınız birindən gəlmiş görünsə belə bir fayl, adamın xəbəri olmadan onun kompüterindən bir virus tərəfindən göndərilmiş ola bilər. Hətta bir e-poçt fərqli bir adamın e-poçt ünvanından gəlirmiş kimi göstərilə bilər. Bu səbəblə tanıdığınız birindən nə olduğunu bilmədiyiniz bir fayl aldıqda, o adama geri dönüb bunu həqiqətən onun göndərib yollamadığını soruşmaq ən doğrusudur. Bundan başqa, son zamanlarda olduqca məşhur olan paylaşım proqramları (Bittorent, Qəzaya, I-Mesh, E-Donkey, DC + + kimi) müəllif hüquqlarını pozan fayllar saxlamaları səbəbiylə tartışılmalarının ilə yanaşı, fərqli adlar altında zərərli fayllar da yerləşdirilir.. Bu vəziyyətdən zərər görməmək üçün də bir anti-virus proqramının aktiv halda saxlanılması vacibdir.

7. ALDATMAÇILARA DİQQƏT EDİN

Gerçək həyatda olduğu kimi İnternet üzərində də insanları aldadaraq və ya qeyri-qanuni işlər etməyə çalışan insanlar vardır. Cəmiyyət mühəndisliyi (social engineering) adı verilən bu davranış ümumiyyətlə insanları aldatmaq və ya xüsusi məlumatlarını ələ keçirmək məqsədi ilə edilir. Xüsusilə sistem idarəçisi olduğunu və müəyyən bir əməliyyatın edilməsi üçün şifrə göndərilməsi lazım olduğunu söyləyən mesajlar, get-gedə daha çox görülən aldadıcı mesajlarıdır. Yemləmə (phishing) deyilən bu tətbiq, bank şifrələrini ələ keçirmək üçün tez-tez istifadə olunur. Bir e-poçtun başqa ünvandan gəlirmiş kimi göstərilməsi də texniki olaraq mümkün olan bir aldatmaca texnikasıdır. Hər vaxt bir məlumatın bir şəkildə dəyişdirilmiş ola biləcəyi və doğru adam tərəfindən gönderilmiyor ola biləcəyi unudulmaması lazım olan bir mövzudur.

İŞİN YERİNƏ YETİRİLMƏ QAYDASI

1. Kompüteri yenilənməyə açıq saxlayın.
2. Kompüterdə istifadə olunan anti- virus proqramını yeniləyin.
3. Yeni poçt ünvanı yaradın. Spam qovluğu ilə tanış olun.
4. Hər hansı bir *İNTERNET* saytından kompüterə bir proqram yükləyin. Proqramın zererli və ya faydalı olduğunu müəyyən edin.

YOXLAMA SUALLARI

1. Kompüterlərinizi yeniləməyə açıq saxlayın dedikdə nə başa düşürsünüz?
2. Kompüterləri viruslardan (ziyanverici proqramlardan) qorumaq üçün hansı proqramlardan istifadə olunur?
3. Poçt ünvanına gələn ziyanverici məktublar hansı qovluqda yerləşir?

LABORATORİYA İŞİ №4
KRİPTOQRAFİYA. SİMMETRİK VƏ ASSİMETRİK ŞİFRƏLƏMƏ

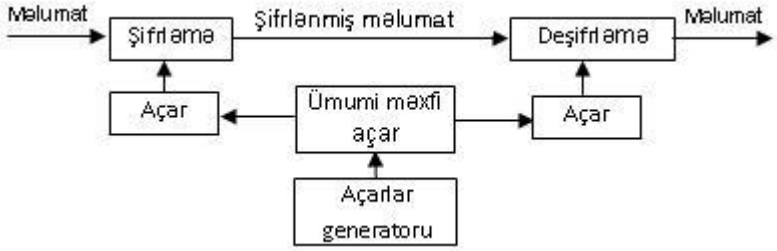
İŞİN MƏQSƏDİ: Şirfələmə haqqında geniş məlumat əldə edərək şıfrələmə üsulları vasitəsilə verilən tapşırığı yerinə yetirmək.

NƏZƏRİ HİSSƏ

Kriptoqrafiya — yunanca *kryptos* (gizli) və *graphos* (yazı) sözlərindən yaranmışdır. Müasir kriptoqrafiyanın predmeti informasiyanı bədniyyətlinin müəyyən əməllərindən mühafizə etmək üçün istifadə edilən informasiya çevirmələridir. Kriptoqrafiya konfidensiallığı, bütövlüyə nəzarəti, autentikasiyanı və müəlliflikdən imtinanın qeyri-mümkünlüyünü təmin etmək üçün tətbiq edilir. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur. Kriptoqrafik alqoritm – məlumatların çevrilməsinin müəyyən üsuludur. Açar isə çevirmə üsulunu konkretləşdirir. Müasir kriptoqrafiya o prinsipdən çıxış edir ki, kriptoqrafik çevirmənin məxfiliyi yalnız açarın məxfi saxlanması ilə təmin edilməlidir. İlk kriptosistemlər artıq bizim eranın əvvəlində meydana çıxır. Məsələn, məşhur Roma sərkərdəsi Yuli Sezar (e.ə. 100-44-cü illər) öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi.

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var:

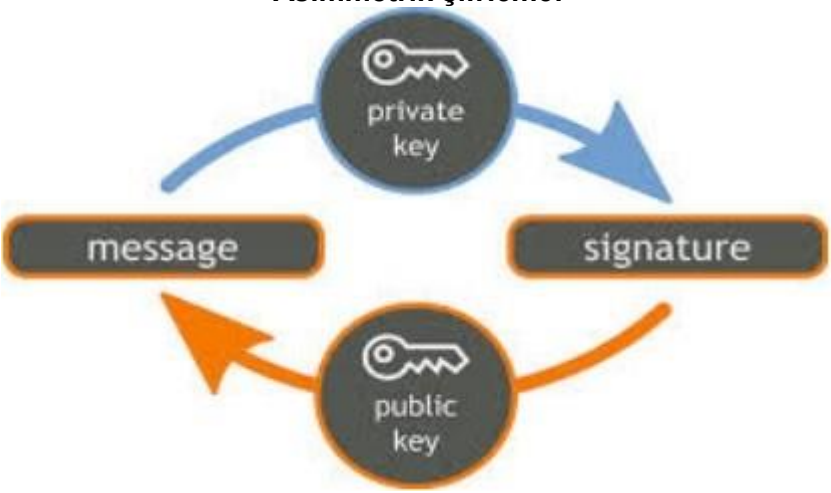
Simmetrik şifrləmə:



Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları var. Simmetrik şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish kimi blok şifrləri və bir sıra axın şifrləri (RC4, A5) daha geniş istifadə olunur.

Əsas nöqsanı: məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Bu bir tərəfdən məxfi açarların tam məxfi kanalla göndərilməsi problemini yaradır. Digər tərəfdən alan tərəf şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən almasını sübut edə bilməz. Çünki belə məlumatı o özü də yarada bilər.

Asimmetrik şifrləmə:



Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar.

Əsas nöqsanı sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla

simmetrik metodla şifrlənir, sonra həmin təsadüfi açarı alan tərəfin açıq asimmetrik açarı ilə şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə, (istifadəçi, açıq açar) cütünün həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün rəqəmsal sertifikatdan istifadə edilir. Rəqəmsal sertifikat xüsusi sertifikasiya mərkəzləri tərəfindən verilir. Rəqəmsal sertifikatda aşağıdakı verilənlər olur: sertifikatın seriya nömrəsi; sertifikatın sahibinin adı; sertifikatın sahibinin açıq açarı; sertifikatın fəaliyyət müddəti; elektron imza alqoritminin identifikatoru; sertifikasiya mərkəzinin adı və s. Sertifikat onu verən sertifikasiya mərkəzinin rəqəmsal imzası ilə təsdiq edilir.

Bütövlüyə nəzarət üçün kriptoqrafik heş-funksiyalar istifadə edilir. Heş-funksiya adətən müəyyən alqoritm şəklində realizə edilir, belə alqoritm ixtiyari uzunluqlu məlumat üçün uzunluğu sabit heş-kod hesablamağa imkan verir. Praktikada 128 bit və daha artıq uzunluqda heş-kod generasiya edən heş-funksiyalardan istifadə edilir.

Heş-funksiyanın xassələri elədir ki, onun köməyi ilə alınan heş-kod məlumatla "möhkəm" bağlı olur. Məlumatın hətta bir biti dəyişdikdə belə heş-kodun bitlərinin yarısı dəyişir. Heş-funksiyaya misal olaraq MD2, MD4, MD5, RIPEMD, SHA1 və s. alqoritmlərini göstərmək olar.

Misal. ‘1234567890’ sətri üçün SHA1 heş-funksiya alqoritminin hesabladığı heş-kod 16-lıq say sistemində 01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A simvollar ardıcıllığıdır.

YOXLAMA SUALLARI

1. Kriptoqrafiya nədir?
2. Kriptoqrafiya anlayışı nə zaman yaranmışdır?
3. Şifrələmənin hansı üsulları mövcuddur?
4. Asimmetrik şifrələmənin iş prinsipini izah edin.
5. Simmetrik şifrələmənin iş prinsipini izah edin.

LABORATORİYA İŞİ № 5
İNKAR EDİLƏ BİLƏN ŞİFRƏLƏMƏ

İŞİN MƏQSƏDİ: İnkar edilə bilən şifrələmənin tədqiq etməkdən ibarətdir.

NƏZƏRİ HİSSƏ

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var:

Simmetrik şifrləmə: Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları var. Simmetrik şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish kimi blok şifrləri və bir sıra axın şifrləri (RC4, A5) daha geniş istifadə olunur.

Asimmetrik şifrləmə: Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar.

İnkar edilə bilən şifrələmə (deniable encryption) — Şifrələnmiş informasiya haqqında tam səlahiyyətli bir adamın ələ keçirilməsi vəziyyətində, qarşı tərəfi aldatmaq üçün istifadə olunan üsuldur.

Bu üsulda ələ keçərilən adam, şifrələmə sisteminin hiyləli açarını söyləyir, qarşı tərəf açarı istifadə edərək sistemdəki açıq məlumata çatdığını zənn edir, ancaq əslində əldə etdiyi məlumat yanlışdır, çünki ona yanlış(hiyləli açar) verilib.

Yuxarıdakı bu vəziyyəti sadə bir nümunə ilə izah edək.

Məqsədimiz iki ədəd açar çıxarmaq və açarlardan birsini gerçək məlumatı açmaq üçün, digərini isə inkar etmək üçün istifadə edək.

Açıq mesaj: SabahMarsda

İnkar mesaj: SabahAyda

Açar: 2

İnkar Açarı: 3

Alqoritm ilk öncə açarla açıq mesajı, daha sonra inkar açarı ilə inkar mesajını şifrələyir. Daha sonra hər iki şifrələnmiş mətni cəmləyərək şifrəli mesajı hasil edir. Şifrələnmiş mətn hər hansı bir yolla ələ keçirlərsə qarşı tərəfi aldatmaq üçün açıq mesajın açar ilə şifrələnmiş halını və inkar açarını verir. Qarşı tərəfdə şifrəli mesajdan bu mesajı çıxaraq yanlış informasiyanı ələ keçirir.

İŞİN GEDİŞİ

1. C++ proqramını işə salmalı.
2. Müəllimin tapşırığı ilə proqramı tərtib etməli.

Alınan nəticəni analiz etdikdə sizə məlum olacaq ki, kodun çıxışından da aydın olacağı üzrə şifrəli mesaj olaraq toplanmış mesaj göndəriləcək. Bu mesajı alan qarşı tərəf mesajı açmaq üçün aşağıdakı düsturu istifadə edəcək:

açıq mesaj = toplanmış - şifrəli inkar - açar

Bu düstur nəticəsində, "SabahMarsda" mesajı alınacaq.

Hər hansı bir şəkildə qarşı tərəfin aldadılması istəndiyində isə aşağıdakı düstur istifadə ediləcək:

inkar mesajı = toplanmış - şifrəli açıq - inkar açarı

Bu düstur nəticəsində, "SabahAyda" mesajı tapılacaq və qarşı tərəf açarları girdikdən sonra tapdığı bu mesajı doğru sanacaq.

YOXLAMA SUALLARI

1. İnkar edilə bilən şifrələmə nədir?
2. Kriptoqrafiya nədir?
3. Şıfrələmənin hansı üsulları var?

C++ kodu

```
#include <iostream>

using namespace std;
void surushdur(char mesaj[], int achar){
   int i=0;
   while (mesaj[i]!='\0'){
   mesaj[i]+=achar;
```

```
    if (mesaj[i]>122)
    mesaj[i]-=26;
    i++;
    }
    }

void topla(char mesaj1[],char mesaj2[]){
    int i = 0;
    while(mesaj1[i]!='\0'){
        int temp = mesaj1[i]+mesaj2[i];
        while(temp>122)
        temp-=26;
        mesaj1[i]=temp;
        i++;
    }
}
int main()
{
    char achiq[100] = "SabahMarsda";
    char inkar[100] = "SabahAyda";
    int achar = 2;
    int inkarachar = 3;
    surushdur(achiq, achar);
    surushdur(inkar, inkarachar);
    printf("Sifreli achiq: %s\n", achiq);
    printf("Sifreli inkar: %s\n", inkar);
    topla(achiq,inkar);
    printf("toplanmis: %s\n",achiq);
}
```

nəticəsi

```
Sifreli achiq: UcdcjOctufc
Sifreli inkar: VdedkDbgd
toplanmis: wyaymywsqfc
```

LABORATORİYA İŞİ №7

Kompüter virusları. Antivirus proqramları vasitəsilə informasiyanın mühafizəsi

İŞİN GEDİŞİ: Laboratoriya şəraitində viruslarla mübarizə usullarını nəzərdən keçirərək, kompüter vasitəsilə verilən tapşırığı yerinə yetirməkdən ibarətdir.

NƏZƏRİ MƏLUMAT

İnformasiyanın qorunması üçün əsas təhlükələrdən biri kompüterə "yerləşmiş" ziyanverici proqramlardır. Belə ziyanverici proqramlar verilənlərin tamlığı üçün təhlükə yarada bilər. ***Kompüterdə saxlanılan verilənlərə və proqramlara zərər vuran proqramlara ziyanverici proqramlar deyilir.***

Əksər ölkələrdə ziyanverici proqramların yaradılması, istifadəsi və yayılması qanunla qadağandır.

Ziyanverici proqramların ən geniş yayılmış növü kompüter viruslarıdır. Kompüter virusu proqramın, sənədin daxilinə, yaxud verilənlər daşıyıcısının müəyyən sahələrinə daxil olan parazit proqram kodudur. Bu kod daxil olduğu kompüterdə özü-özünü çoxalda, müxtəlif icazəsiz və ziyanlı işlər görə bilər.

Özü-özünü çoxaltma qabiliyyəti virus proqramlarının başlıca xüsusiyyətidir. Bu proqramlar kompüter və digər daşıyıcıların sahiblərinin xəbəri olmadan öz nüsxələrini yaradır. Bir çox viruslar ziyan vurmaqla - verilənləri məhv etmək və kompüterin normal işini pozmaqla da məşğul olurlar. Öz bioloji "qardaşları" kimi, kompüter viruslarının arasında da elələri vardır ki, onlar öz-özünə çoxalıb yayılır, lakin heç bir ziyan vurmur.

Kompüterdə virusun "həyat yolu" yoluxdurma və aktivləşmə ilə başlanır. Yoluxma təxminən bu cür baş verir: istifadəçi öz kompüterində virus daşıyıcısı olan proqramı başladır. Bu proqram İnternetdən də "yüklənə" bilər, tanışlarınızdan köçürüb əldə etdiyiniz proqram da ola bilər. Proqramın yüklənməsindən əvvəl, yaxud sonra virus aktivləşərək fəaliyyətə başlayır. Virusun fəaliyyət ssenarisi təxminən belə olur:

1. Kompüterdə yoluxdurulması mümkün olan bütün proqramları tapmaq.
2. Özünü proqramın əvvəlinə, yaxud sonuna yazmaq.
3. Əgər "kritik" tarix, başqa sözlə, virusun hücuma keçəcəyi gün yetişmişsə, dağıdıcı işlər görmək.

4. Əgər həmin tarix yetişməmişsə, hər hansı "xırda" zərər yetirmək; məsələn, kompüterin sərt diskində hər hansı kiçik sahəni "şifrləmək".

"Kompüter virusu" termini ilk dəfə 1973-cü ildə "Westworld" fantastik filmində istifadə olunmuşdur. Həmin filmdə bu sözbirləşməsi məhz bugünkü anlamda işlədilmişdir: "Kompüter sisteminə geniş yayılmış ziyanverici proqram".

Bəs kompüterin virusa yoluxmasını necə müəyyən etmək olar? Kompüterə ziyanverici proqramların girməsini bildirən bir sıra əlamətlər vardır:

* ekrana nəzərdə tutulmamış məlumatların və görüntülərin çıxması;
* nəzərdə tutulmamış səs siqnallarının verilməsi;
* CD/DVD disksürəninin özü-özünə açılması və bağlanması;
* kompüterdə hər hansı proqramın "özbaşına" başladılması;
* kompüterin tez-tez sıradan çıxması və "ilişməsi";
* proqramlar başladılarkən kompüterin yavaş işləməsi;
* fayl və qovluqların yoxa çıxması, yaxud dəyişdirilməsi;
* sərt diskə tez-tez müraciət;
* brauzerin asılıb-qalması, yaxud özünü gözlənilməz aparması (məsələn, proqram pəncərəsini qapatmağın mümkün olmaması).

İnternetin inkişafı virusların da yayılma sürətinə güclü təsir göstərdi. Bundan başqa, viruslar "keyfiyyətcə" də dəyişdi. Əgər təxminən 10-15 ilbundan öncə virus müəlliflərinin əsas məqsədi kompüteri sıradan çıxarmaq idisə, XXI əsrin əvvəllərində virusların başlıca fəaliyyəti düşdüyü kompüterdən hər hansı informasiyanı oğurlamağa və həmin kompüterə kənar şəxslərin daxil olmasını təmin etməyə yönəlmişdir. İnformasiyanı oğurlayan virus hər hansı bir şirkətin gizli saxlanılan sənədlərini açıqlamaqla, həmin şirkətin nüfuzuna ciddi zərbə vura bilər. Əgər belə virus məxfi hərbi sənədlərin, yaxud başqa sirlərin olduğu kompüterə düşərsə, nə baş verəcəyini təsəvvür etmək belə çətindir.

Dünyanın inkişaf etmiş ölkələrində kompüter viruslarının vurduğu ziyan yüz milyon dollarlarla ölçülür.

Ziyanverici proqramların yarandığı dövrlərdə, sadəcə, istifadəçilərin işinə mane olan zarafat-viruslar daha populyar idi. Məsələn, bir virus proqramı ekrana belə məlumat çıxarırdı: "L + A + M + E + R + F1 + Alt klavişlər kombinasiyasını eyni zamanda basın". İstifadəçi bu "məsləhətə" əməl edən kimi məlumat verilirdi ki, faylların yerləşmə cədvəli sərt diskdən silinərək, operativ yaddaşa yazıldı və əgər istifadəçi barmağını hər hansı bir klavişin üzərindən götürərsə, o, sərt diskdəki informasiyalarla vidalaşmalı olacaq. Yox, əgər düz bir saat bu vəziyyətdə gözləyə bilsə, hər şey əvvəlki vəziyyətinə qayıdacaq. Bir saat bu cür vəziyyətdə qaldıqdan sonra məlum olurdu ki, bu bir zarafat imiş.

Virus proqramlarının ən ziyanlı növlərindən biri Troya proqramlarıdır. Troya proqramları istifadəçidən icazəsiz olaraq informasiyaları toplayır və onları "cinayətkara" göndərir, eləcə də həmin informasiyaları dağıdır, yaxud ziyanlı məqsədlər üçün dəyişdirir. Bundan başqa, Troya proqramları kompüterin işini poza bilər, yaxud istifadəçidən xəbərsiz olaraq kompüterin resurslarından ziyanlı məqsədlər üçün istifadə edə bilər.

Troya virusları öz adını bir tarixi hadisədən götürüb. Homerin "İliada" poemasında qədim yunanlar tərəfindən Troya şəhərinin mühasirəsi (e.ə. təxminən 1250-ci ildə) təsvir olunub. Yunanlar taxtadan nəhəng at düzəldib, içərisinə öz döyüşçülərini yerləşdirmiş və onu şəhər darvazasının qabağında qoymuşlar. Heç nədən şübhələnməyən troyalılar atı çəkib darvazadan içəri salmış, ancaq gecə yunan döyüşçüləri atın içərisindən çıxıb, şəhəri tutmuşlar.

Troya proqramları, adətən, kompüterə şəbəkə soxulcanı kimi girir. Onlar bir-birindən öz "əməllərinə" görə fərqlənir.

*** Uzaqdan idarəetmə utilitləri.** Bu qrupa aid proqramlar şəbəkədə olan kompüteri uzaqdan idarə edən utilitlərdir. Belə gizli idarəetmə utilitləri faylları qəbul edə, yaxud müxtəlif ünvanlara göndərə, onları başlada və məhv edə, kompüteri yenidən yüklədə bilər və s.

*** Casuslar.** Bu qrupa aid troyalılar elektron casusluqla məşğul olurlar: yoluxmuş kompüterdə istifadəçinin klaviaturadan daxil etdiyi informasiya, ekranın şəkli, aktiv proqramların siyahısı və istifadəçinin həmin proqramla yerinə yetirdiyi əməllər müəyyən fayla yazılır və vaxtaşırı "cinayətkara" göndərilir. Bu tipli Troya proqramlarından çox zaman bank və onlayn ödəmə sistemlərinin istifadəçiləri haqqında məxfi informasiyaların oğurlanması məqəsədilə istifadə olunur.

* **Reklam proqramları.** Reklam proqramları (ing. Adware: Advertisement - reklam və Software - proqram təminatı) hər hansı bir proqrama reklam kimi yerləşdirilir və Troya casus proqramı funksiyasını yerinə yetirə bilir. Reklam proqramları gizlicə kompüterin istifadəçisi haqqında müxtəlif informasiyalar toplaya, sonra onu "cinayətkara" göndərə bilir.

Virus hücumlarının təsirini heçə endirməyin ən uğurlu yolu mühüm əhəmiyyət kəsb edən verilənlərin ehtiyat üçün surətlərinin saxlanmasıdır.Viruslar aparat vasitələrini sıradan çıxara bilmir. Virus hücumlarının əlamətləri aşkarlandıqda kompüterin verilənlər daşıyıcılarını büsbütün təmizləmək lazımdır. Verilənlərin ehtiyat daşıyıcılardan köçürülməsi kompüter sisteminin normal vəziyyətini bərpa etməyə imkan verir.

Kompüterdə virus əlamətləri aşkarlandıqda nə etməli? İlk addım olaraq yerinə yetirdiyiniz işlərin nəticələrini xarici daşıyıcıda (disketdə, CD- və ya DVD-diskdə, fləş-kartda və s.) saxlayın. Sonra

* kompüteri lokal şəbəkədən və İnternetdən ayırın (əgər qoşulmuşsa);

* əməliyyat sistemi kompüterə düşmüş virus nəticəsində sərt diskdən yüklənmirsə, onda onu CD diskdən yükləməyə çalışın;

* antivirus proqramını başladın.

Antivirus proqramları vasitəsilə informasiyanın mühafizəsi. Kompüter virusunun öz bioloji "qardaşı" ilə bir oxşarlığı da əvvəlcədən hər ikisinin qarşısının alınmasının (profilaktikasının), yoluxmadan sonrakı müalicəyə nisbətən çox-çox asan olmasıdır. Kompüter viruslarından qorunma üç səviyyədə təşkil oluna bilər:

Birinci səviyyədə virusların kompüterə girməsinin qarşısı alınır.

İkinci səviyyədə virus hücumlarının qarşısı alınır.

Üçüncü səviyyədə virus hücumlarının təsiri minimuma endirilir.

Təhlükəsizlik tədbirləri nəticəsində virusların kompüterə düşməsi təhlükəsi azaldılır. Şübhəli mənbələrdən əldə olunan proqram təminatlarından istifadədən qaçmaq lazımdır. Kompüterə kənardan, o cümlədən İnternetdən daxil olan proqram koduna çox ciddi nəzarət olunmalıdır.

Yoluxma faktını aşkarlamaq, virusların çoxalmasına mane olmaq və virus hücumlarının qarşısını almaq üçün antivirus proqramlarından istifadə olunur. Verilənlərin mübadiləsi zamanı viruslara xas olan baytların aşkar edilməsi və viruslar üçün xarakterik hərəkətlərin qeydə alınması onların axtarışının əsasını təşkil edir.

Müqayisə üçün zəruri olan verilənlər antivirus proqramının verilənlər bazasında saxlanılır. Antivirus verilənlər bazasını daim yeni viruslar haqqında məlumatlarla doldurmaq, başqa sözlə, virus bazasını yeniləmək lazımdır. Antivirus proqramlarının uğuru da məhz bundan asılı olur.

Fəaliyyətlərindən asılı olaraq antivirus proqramları bir neçə sinfə ayrılır:

*** Detektorlar** hər hansı məlum virusa yoluxmuş faylları aşkarlamağa imkan verir.

*** Doktorlar (faqlar)** təkcə yoluxmuş faylları aşkarlamır, həm də onları ilkin duruma qaytarmağa çalışır.

*** Müfəttişlər** kompüter hücumları mümkün olan yerlərdəki dəyişikliklərə nəzarət edir; bu məqsədlə proqramların və disklərin sistem sahələrinin ilkin, yoluxmamış hesab edilən durumları haqqında məlumat yadda saxlanılır, sonra istifadəçinin müəyyən etdiyi vaxtda onları cari vəziyyətlə müqayisə edir.

*** Doktor-müfəttişlər** yuxarıda göstərilən iki növ proqramın imkanlarını özündə birləşdirir.

*** Süzgəclər** virusların çoxalma və zərərvurma məqsədi ilə əməliyyat sisteminə etdikləri müraciətləri tutur.

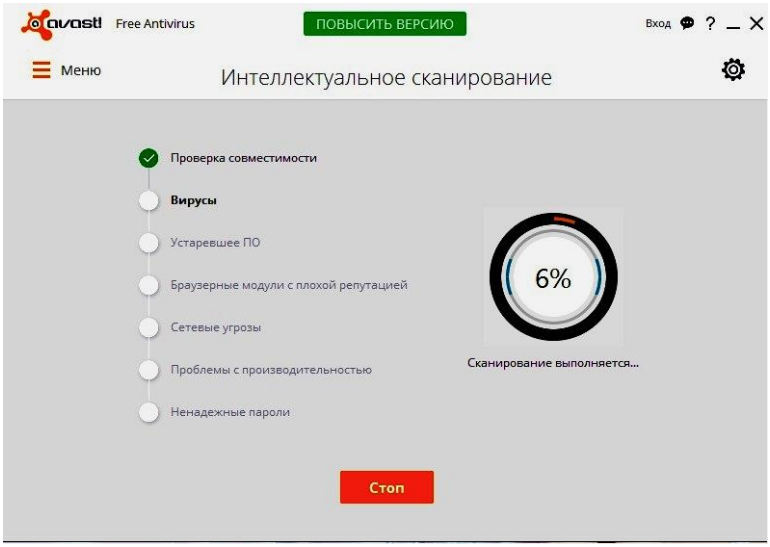
*** Vaksinlər**, yaxud immunizatorlar iş qabiliyyətlərini saxlamaqla proqramları elə dəyişdirirlər ki, onlar viruslar üçün yoluxmuş kimi görünsün. Belə olduqda, viruslar həmin fayllara "ilişmir".

Kompüterdə virusların axtarışı verilənlər daşıyıcılarının, yaxud axınının daranması [scan] yolu ilə yerinə yetirilir. Darama prosesində operativ yaddaşda, daşıyıcılarda virusa yoluxmanın əlamətlərinin olub-olmaması yoxlanılır. Aşkarlanmış viruslar deaktivləşdirilir və məhv edilir. Mümkün olduqda dəyişdirilmiş (yoluxmuş) faylların ilkin vəziyyəti bərpa olunur.

Bu gün Symantec Norton Antivirus, Kasperski antivirusu, Dr. Web, AcAfee VirusScan, Panda Titanium Antivirus kimi antivirus proqramları daha çox tanınır.

İŞİN GEDİŞİ

1. Kompüteri işə salmalı.
2. Kompüterlə şəbəkə arasında əlaqə yaratmalı.
3. Müəllimin tapşırığı ilə İnternetdən antivirus proqramı yükləməli. (şəkil -1)
   http://www.comss.ru/
4. Yüklədiyiniz proqramı işə salmalı.
5. Antivirus proqramını aktiv hala gətirməli.(şəkil-3)



YOXLAMA SUALLARI

1. Ziyanverici proqramlar nəyə deyilir?
2. ***"Kompüter virusu"*** termini ilk dəfə nə vaxt yaranıb?
3. Kompüterdə virus əlamətləri aşkarlandıqda nə etməli?
4. Virus proqramlarının en təhlükəli və geniş yayılan növü hansıdır?
5. Hansı antivirus proqramını tanıyırsınız?

LABORATORIYA IŞİ №7
İNFORMASİYANIN ARXİVLƏŞDİRİLMƏSİ VƏ EHTİYYAT SURƏTLƏRİNİN YARADILMASI SİSTEMLƏRİ

İŞİN MƏQSƏDİ: Bu işdə əsas məqsəd informasiyanın arxivləşdirilməsi və ehtiyyat surətlərinin yaradılması məsələlərini tədqiq etməkdən ibarətdir.

ƏSAS NƏZƏRİ MƏLUMATLAR

Etibarli və səmərəli arxivləşdirmə sisteminin təşkili kompüter sistemlərində və şəbəkələrində informasiyanın qorunması, tamlığının, ona icazəli girişin təmin edilməsi və onun təcrid olunmasının qarşısının alınması üzrə ən vacib məsələlərindən biridir. Bir və ya iki server quraşdırılmış şəbəkələrdə arxivləşdirmə çox vaxt bilavasitə serverdə olan sərbəst slotlara quraşdırılır. Daha böyük korporativ şəbəkələrdə ayrıca xüsusiləşdirilmiş arxivləşdirmə serverinin təşkil olunması daha məqsədəuyğun hesab olunur.

Əlahiddə qiymətə malik olan arxiv informasiyasının saxlanması xüsusi qorunan otaqda təşkil olunmalıdır. Mütəxəssislər yanğın və ya digər təbii fəlakətlərin baş verməsinin mümkünlüyünü nəzərə alaraq, daha qiymətli məlumatların arxivləşdirilməsi ikinci surətinin başqa binada saxlanılmasını tövsiyyə edirlər.

Arxiv proqramları (Arxivatorlar) - fayldakı informasiyları sıxmaqla onların arxivləşməsini yerinə yetirir. Sıxma dərəcəsi asılıdır:

1. İstifadə olunan arxivatordan
2. Sıxma üsulundan
3. Faylın tipindən.

Arxivləşdirmənin iki səbəbi var:

1. İnformasiyanın qorunması (faylın rezerv surətini yaratmaqla)
2. Fayllar üçün ayrılmış yerdən səmərəli istifadə.

Arxivləşmə zamanı faylın daha kiçik həcmə malik, rezerv surəti yaradılmış olur.

Rezerv surət – faylın dəqiq surəti olub, sıxılmış halda xüsusi daşıyıcıda, təhlükəsiz yerdə saxlanılır.

Arxiv faylları: ARJ, CAB, GZ, LHA, RAR, TAR, TGZ, UU, ZIP.

Windows əməliyyat sistemlərində əsasən WinZİP və WinRAR arxivatorlardan istifadə edilir.

İŞİN GEDİŞİ:

Aşağıda göstərilən internet ünvanlarının hər hansı birindən arxiv proqramını yükləyin.

- http://www.win-rar.ru/download/
- http://www.7-zip.org/
- http://www.winzip.com/
- http://www.rarsoft.com/

-Proqramı işə salmaq üçün:

1. Start (Старт) → Proqrams (Программы) → WinRAR → [Bakcomp – WinRAR] pəncərəsi açılır → arxivləşdirilməsi lazım olan fayl və ya qovluq açılan pəncərədə göstərilir → [Добавить] düyməsi basılır.
2. Fayl və ya qovluğun üzərində kontekst menyu açılır → «Добавить в Архив…» əmri verilir → açılan [Имя и параметры архива] pəncərəsində arxiv faylın yerləşəcəyi qovluq göstərilir → OK.

Arxiv olunacaq fayl və ya qovluğa parol qoymaq üçün: [Имя и параметры архива] pəncərəsində [Дополнительный] hissəsinə keçilir → [Установить пароль] →[Архивация с паролем] pəncərəsində parol təyin edilir → OK.

YOXLAMA SUALLARI

1. Kompüter sistemlərində informasiyanın arxivləşdirilməsi nə üçün lazımdır?
2. Hansı arxiv proqramlarını tanıyırsınız?
3. Yaddaş kartında gizlənmis informasiyanı necə və neçə üsulla geri qaytarmaq olar?